

シングルサインオンによるGléas UAログイン

(VMware Workspace ONE Access 連携)

Ver.1.0

2023 年 3 月

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

- JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の 国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。 Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- · その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

目次

1.	はじる	りに5
	1.1.	本書について5
	1.2.	本書における環境
	1.3.	本書における構成
2.	AD Ø)設定
	2.1.	SSL 証明書をインポート8
3.	Gléas	; アカウントの登録11
	3.1.	AD ユーザ情報をインポート11
4.	SAM	L SP 署名用証明書の発行14
5.	WS1	Access の設定16
	5.1.	AD ユーザ情報を同期16
	5.2.	ID プロバイダの作成
	5.3.	ユーザーグループの作成24
	5.4.	Web アプリケーションの登録
	5.5.	Web アプリケーションの割り当て

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)
6. Gléas の管理者設定 (Windows 向け)33
7. クライアントからのアクセス (Windows)36
7.1. シングルサインオンで UA にログイン
7.2. クライアント証明書のインポート
8. Gléas の管理者設定 (iPhone 向け)40
9. クライアントからのアクセス (iPhone)44
9.1. シングルサインオンで UA にログイン44
9.2. クライアント証明書のインポート46
10.Gléas の管理者設定(Android 向け)49
11. クライアントからのアクセス (Android)54
11.1. シングルサインオンで UA にログイン54
11.2. クライアント証明書のインポート56
12.問い合わせ

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベート認証局 Gléas」のユーザ申込局 UA を、VMware Workspace ONE Access (旧称 VMware Identity Manager)のWebアプリケーショ ンとして登録し、シングルサインオンで UA にログインする環境の設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環 境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例とし てご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、 最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- SAML IDP: VMware Workspace ONE Access (旧称 VMware Identity Manager)
 ※以後「WS1 Access」と記載します
- > SAML SP: JS3 プライベート認証局 Gléas (バージョン 2.6.0) UA
 ※以後「UA」と記載します

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- ドメインコントローラ: Microsoft Windows Server 2019
 ※以後「AD」と記載します。
 ※WS1 AccessとのID同期には、Workspace ONE Access Connectorを使用しています。
- > JS3 プライベート認証局 Gléas (バージョン 2.6.0)
 ※以後「Gléas」と記載します
- クライアント: Windows 10 Pro (21H1) / Microsoft Edge 104.0.1293.70
 ※以後「Windows」と記載します
- > クライアント: iPhone X (iOS 16) / Safari

※以後「iPhone」と記載します

以下については、本書では説明を割愛します。

- WS1 Accessの基本設定、およびADとのID同期方法
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- Windows、iPhone での UA へのログイン方法

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている

販売店にお問い合わせください。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



- 1. Windowsでは、EdgeブラウザからUAへアクセス試行する
- 2. 認証連携先のWS1 Accessのログイン画面に画面遷移。WS1 Accessはパスワードを

要求し、認証成功するとUAにログインした状態になる

- 3. iPhoneでは、SafariブラウザからUAへアクセス試行する
- 4. 認証連携先のWS1 Accessのログイン画面に画面遷移。WS1 Accessはパスワードを

要求し、認証成功するとUAにログインした状態になる

- 5. Androidでは、ChromeブラウザからUAへアクセス試行する
- 6. 認証連携先のWS1 Accessのログイン画面に画面遷移。WS1 Accessはパスワードを

要求し、認証成功するとUAにログインした状態になる

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

2. AD の設定

2.1. SSL 証明書をインポート

ADにSSL証明書をインポートして、LDAPSを有効化します。

ADサーバのFQDNが記載されたSSL証明書を準備します。

※SSL証明書はGléasから発行することも可能です。詳しくはお問い合わせください。

PKCS#12(.pfx)形式の SSL 証明書を AD サーバにコピーします。

MMC を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明 書]を追加します。

「証明書のスナップイン」では、[サービス アカウント(S)]を選択し、

次の「コンピューターの選択」では、[ローカルコンピューター(L)]を選択し、

次の「証明書スナップイン」では、[Active Directory Domain Services)]を選択し、

[完了]をクリックします。

証明書スナップイン	× コンビューターの歴史		×	証明書スナップイン		×
2021/9/27世間9年2月巻 - 3:4-7702740 その - 3765-9-7702746 - 3765-9-7702746	2003/57/2118 2003/57/2718 @ to to 2018 0 Nov2712-2 0 Nov272-2 2702.2019	NY 2016-9-128, (120), NY 2016-27-1 NY 2016-2017-1488,(10,000/2-7-) NY 2016-2016-2016-2016-2016 NY 2016-2016-2016-2016-2016 NY 2016-2016-2016-2016-2016 NY 2016-2016-2016-2016	15 M ₁₀	D-ds.5/2-P-1488739-230757714887 P-427757110 Mater Dampy Cellstrate Service Mater Dampy Cellstrate Service Mater Dampy Cellstrate Service All Cell	n 1. rosu	
< #(3(3)	2/(N) > キャンセル	< #3(3) 32A(N) >	キャンセル		< 戻る(8) 完了 キャンセル	

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

スナップインが追加されたら左ペインより[証明書-ローカルコンピューター上のサービス] > [NTDS ¥ 個人]と展開し、中央ペインで右クリックして、[すべてのタスク(K)] > [インポート(I)]をクリックします。

「証明書のインポートウィザード」が開始されるので、SSL 証明書をインポートしま

 \times

次へ(N) キャンセル

す。

÷ 🐉	証明巻のインボートウィザード
	証明書のインポート ウィザードの開始
	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。
	証明機関によって発行された証明會は、ユーザーIDを確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接触を提供するための情報を含んでいます。証明音ストアは、証明音が保留されるシステ ム上の領域です。
	保存場所
	○ 現在のユーザー(C)
	・ ローカル コンピューター(L)
	続行するには、[次へ] をクリックしてください。

ページ	設定
証明書のインポートウィザードの開始	[次へ(N)]をクリック
インポートする証明書ファイル	SSL 証明書ファイル (拡張子 : p12/pfx) を指定し
	て、[次へ(N)]をクリック
秘密キーの保護	SSL 証明書のパスフレーズを入力して、[次へ(N)]
	をクリック
証明書ストア	[証明書をすべて次のストアに配置する(P)]を選択
	し、[証明書ストア]に[NTDS¥個人]が指定されて
	いることを確認し、[次へ(N)]をクリック
証明書インポートウィザードの終了	[完了(F)]をクリック

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

中央ペインで右クリックして、[最新の情報に更新(F)]をクリックします。

左ペインより[証明書-ローカルコンピューター上のサービス] > [NTDS ¥ 個人] > [証明

書]と展開すると、インポートされた証明書が確認できます。

※中央ペインにルート証明書がある場合には、ルート証明書を選択し、左ペインの[証明書-ローカルコ ンピューター上のサービス] > [NTDS¥信頼されたルート証明機関] > [証明書] に移動してください。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

3. Gléas アカウントの登録

3.1. AD ユーザ情報をインポート

AD のユーザ情報を LDAPS で Gléas のアカウントとしてインポートします。

GléasのRA (登録局) にログインします。

[アカウント]>[アカウント新規作成]メニューから[上級者向け設定」をクリックします。

▶アカウント情報			□ 上級者向け設定
> アカウント名 📩			
▶初期グループ		tau	
		■ここをクリックしてユーザを参加させるグループを選択	
> その他の設定		□ 証明書を発行する	
		□ 連続して登録を行う	
▶種類 ○ ユー!	げ 0 コンピ	ュータ 〇 サーバ 〇 認証局 〇 CSVファイルー括登録 🖲 LDAP	
> 指定方法		○ URL ◉ ホスト名	
> ホスト名		10.00.0	
>ポート番号		636	
> Base DN		OU= ,DC= ,DC= ,DC=	
> 管理者DN		CN= ,CN= ,DC= ,DC= ,DC=	
>パスワード			
> 検索フィルタ		(objectClass=person)	
> グループメンバー	- 属性		
> 前回のインポート	ŀ	1970/01/01 09:00 🗹 前回のインボート以降に作成されたエントリのみ	
> 属性のマッピング	Ï	カスタム設定	
Gléasの属性		LDAPの属性	
アカウント名	userPrincipa	IName	
名前(姓)	sAMAccount	Name	
名前(名)	givenName		
メールアドレス	mail		
パスワード			
プリンシバル名	userPrincipa	IName	
		(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	

- [▶種類]から[LDAP]を選択
- [指定方法]に[ホスト名]を選択
- [ホスト名]に AD のホスト名を入力

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- [ポート番号]に "636" を入力
- [BaseDN]にユーザ情報の検索対象となるベース DN を入力
- [管理者 DN]に BaseDN 以下にアクセスできる AD 管理者の DN を入力
- [パスワード]に AD 管理者のパスワードを入力
- [検索フィルタ]に "(objectClass=person)" を入力
- [属性のマッピング]に[カスタム設定]を入力
- [Gléas の属性]に Gléas のアカウントと LDAP 属性の紐づけを入力

Gléas の属性	LDAP の属性		
アカウント名	userPrincipalName		
名前 (姓)	sAMAccountName		
名前 (名)	givenName		
メールアドレス	mail		
パスワード	空欄		
プリンシパル名	userPrincipalName		

● [作成]をクリック

	~Herry 7 JUJ/13	2詠甲請者一覧に反F	快されます。	
ァイルの最初の4件 アカウント名	妙生	名	メールアドレス	プリンシバル名
10 March 10				10.000.000.000.000

● 内容を確認し[実行]をクリック

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

[アカウント]>[登録申請者一覧]メニューを選択します。

※しばらくするとアップロードしたユーザ情報がアカウント登録申請として登録されます。



- [すべて許可する」をクリック
- [実行]をクリック

これで AD のユーザ情報が Gléas のアカウントとしてインポートされました。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

4. SAML SP 署名用証明書の発行

SAML SPとして使用する署名用証明書をGléasから発行します。

GléasのRA (登録局) にログインします。

[アカウント]>[アカウント新規作成]からアカウント saml_sp を作成します。

🕂 新規アカウント作成		
アカウント情報の入 このページではアカウントの新規 アカウントは証明書を発行する対 ☆の付いている項目は入力必須	ー 力 作成を行います。 象(エンドエンティティ)のことで、このページで指定したアカウント名が証明書の発行先と 項目です。	北山ます。
▶アカウント情報		● 上級者向才設定
>アカウント名 🚖	saml_sp	
>名前(姓) 対	SAML	
>名前(名) 📩	SPi证明書	
>メールアドレス		
>パスワード		
>パスワード(確認)		
>バスワード(自動生成)	パスワード生成	
>プリンシバル名		
	(теру	

[証明書発行]で saml_sp アカウントに対し証明書を発行します。

Saml_sp		
東証明書発行 この画面では証明書要求の作成さ行います。 た例の「サブジェクト」と「高性」の内容で証明書要求を作成します。 右側のテンブレートの中から必要なものを選択して「発行」を押してください。		
▶ 正明書発行 ▶ 下記の内容で証明書を発行します。よろしければ「発行」を押してください。	- Rit	★上級者向丁設定
▶ॻॖॻॖॻ॒ॻॖ	▶選択されているテンプレート	■全工解除
> CN=samI_sp > 0=JCCH Security Solution Systems > DC=local, jcch-sss	 > 必須 デフォルト設定 > 必須 区分CRL 	
▶届性	> なし	
 > 発行局: > 調告アルニリンズム: RSA暗号 > 課長: 2048bit > タイジェストアルゴリンズム: SHA256 > 有効日数: 1年 > 線用論:: 電子署名, 鍵の暗号化 > 拡張線用論: SSLグライアント認証 > Netscape 拡張: 有効 > CRL 配布点: 		

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

証明書詳細画面から[ダウンロード]をクリックし証明書をダウンロードします。

(証明書情報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
▶ <u>sami_sp</u>	開始日:2022/09/28 10:09 終了日:2023/09/28 10:09
▶ 説明:	最終更新:2022/09/28 10:10 <mark>編集</mark>
▶₩	▶基本情報
→ 一般名:sam_sp 組羅:JCCH Security Solution Systems ドメインコンボーネント:local ドメインコンボーネント:locals) 作成日:2022/09/28 10:08 > 有加日数:365 > 失功日: > 失功理由: > 判認除于日: > 対能:有加は証明書 > 処理の状態:有加は証明書 > トーヴン必要:
2日現在前期 (2015年): 昭号アルビリズム: 15日 ダジェスト・アルニリズム: 5日の256 連長: 2048 (2015年): 連手工会: 2020年1月): 日本の1000年1月): 日本の1000年1月):	
 ■ 正明書稿稿 ● 正明書 ● ジョント・レージズム: sna255 ● ジョント・レージズム: sna255 ● 屋田浩: 電子電台 ● 図田油: 電子電台 ● SLクラ・イアント2020 ● SNA: 	

※ダウンロード時に証明書、秘密鍵を取り出す際のパスフレーズを指定します。

ダウンロードした.p12ファイルからPEM形式の証明書を取り出します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

openssl pkcs12 -in saml_sp.p12 -out saml_sp.crt -nokeys -clcerts openssl x509 -in saml_sp.crt -out saml_sp.crt

※取得した証明書ファイル saml_sp.crt を保存します。

ダウンロードした.p12ファイルからPEM形式の秘密鍵を取り出します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)



※取り出した秘密鍵ファイル saml_sp.key を保存します。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

5. WS1 Access の設定

5.1. AD ユーザ情報を同期

AD のユーザ情報を WS1 Access に同期します。

【Workspace ONE Access Connector をセットアップ】

ドメイン参加している Windows サーバに Workspace ONE Access Connector をイ

ンストールし、WS1 Access と接続します。



シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

【ディレクトリを追加】

Workspace ONE Access コンソール にログインします。

メニュー [統合] > [コネクタ] > [ディレクトリ] を選択します。

[ディレクトリを追加] > [Active Directory] をクリックします。

- [ディレクトリ名] に任意のディレクトリ名を入力
- [LDAP 経由の Active Directory] を選択
- [ディレクトリ同期ホスト] に同期対象 AD ホストをチェック
- [認証] に [はい] を選択
- [ユーザー認証ホスト] に同期対象 AD ホストをチェック
- [ユーザー名] に [userPrincipalName] を選択
 ※AD の userPrincipalName が Workspace ONE Access のユーザ名となります
- [外部 ID] に "objectGUID" を入力

※Workspace ONE Access ディレクトリ内ユーザの一意の ID として使用する属性

- [このディレクトリ は DNS サービス ロケーションをサポートします] のチェッ クを外す
- [サーバ ホスト名] に 同期対象 AD の FQDN を入力
- [サーバ ポート] に "636" を入力
- [すべての接続に必要な LDAPS] をチェック

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- [SSL 証明書] に PEM 形式で LDAPS の証明書チェインを貼り付け
 ※サーバ証明書 > 中間証明書 > ルート証明書の順
- [ベース DN] に 同期対象となる DN を入力
- [バインド ユーザー DN] にベース DN にアクセスできる管理者 DN を入力
- [バインド ユーザー パスワード] にベース DN にアクセスできる管理者パスワー

ドを入力

ドイレクトリ名	100000000000000000000000000000000000000		5-7004678	ックボックスをオンにします し、Active Directory サーバ	DNS SRV ルックアップを使用しない場合は、チェックボックスを進行解除 れスト名とボート巻号を入力します。
ディレクトリの阿弗と認証	 LDAP 経由の Active D ・ 税会 Windows 総量を) Active Directory から Winese Active Directory 周期ホスト・ ディレクトリ周期ホスト・ 	instony 男子する Active Directory 明 Whatpace ODE Access ジィレクトリにユーザーを配成するのなくとを1つの 空間パルタマ・ (アクティブ)		□ このディレクトリ は D □ このディレクトリには. サーバホスト名・ サーバポート*	N5 サービス ロケーションをサポートします グローバル カケログガタウます 636
	第22 ユーザー認知ホスト・ ユーザー名。		编号化	すべてのディレクトリ扱法の ▼ すべての総告に必要な ドメインコントローラのルー SOL 証明書。	バレビ 58/パト5 生物にとする LCAPS ト へく見込まった知知時日(原用する場合) で入力します。 - の日の地やパードロンパーをついたので、100/mmp/0.get 100 mm 200 mm の日代地やパードロンパーをついたので、100/mm 100/mm/0.016/mg/date - 一日の COETTIOLTE
	91∰) ID1	ebject/GUID Warkspace ONE Access ディレクトリ内のユーザーの一帯の ID として使用す る時に、			まれ、 - 経時巻を PEM 形式で入力する - ルート CA 証明者の和に中國証明者を入力する - BEGIN CERTIFICATE の互切り行を含める - すべての中間ルート CA 証明書チェーンを含める
サーバの場所	DNS サービス ロケーション ックボックスをオンにします し、Active Directory サーバ	(SRV)レコードを使用して Active Directory ドメインを特定するには、このチェ F、DNS SRV /レックアップを使用しない場合は、チェックボックスを運用解除 ホスト名とボート毎号を入力します。	バインド ユーザーの詳細	(ベースDNJ フィールドに、) OU=myUnit_DC=myCorp.DC カウントを入力します。たと	Pカウント検索を開始する説明名 (DN) を入力します。たとえば、 soom です、 U (インドユーザー DNI フィールドには、ユーザーを検索できるア Rifs、ON-user1,ON-Uses, OU-enyUnt,DC-enyCore,DC+com です。
	このディレクトリは	DNS サービス ロケーションをサポートします		X-Z DN'	OU= .DC= .DC= .DC=
	このディレクトリには	L. グローバリレカタログがあります		バインドユーザー DN*	CN= DC= DC= DC=
	サーバホスト名*	and an early and early and		バインドユーザーバスワ ード	
	サーバポート*	636			Active Directory のバインド アカウント パスワードを入力します。

[保存と設定] をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

【ディレクトリ同期設定】

メニュー [統合] > [コネクタ] > [ディレクトリ] を選択します。

作成したディレクトリ名のリンクをクリックします。

[同期設定]をクリックします。

[同期サービス] タブを選択します。

● [同期サービス] に同期対象ディレクトリが指定されていることを確認



[ドメイン] タブを選択します。

- [すべてのドメインを取得] の右の [©] アイコンをクリック
- [ドメイン] に 同期対象のドメイン名が表示されることを確認



シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

[マップされた属性] タブを選択します。

- WS1 Access と AD の LDAP 属性のマッピングを確認、修正
 - ※以下は検証時に指定した値

VMware Workspace ONE Access の属性名	Active Directory の属性名
userPrincipalName	userPrincipalName
username	userPrincipalName
distinguishedName	distinguishedName
Disabled	userAccountControll
domain	canoricalName
email	mail
employeeID	employeeID
firstName	givenName
lastName	sn
objectGUID	objectGUID
Phone	telephoneNumber
sourceAnchor	objectGUID



シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

[グループ] タブを選択します。

● [ネストされたグループ メンバーを同期] をチェック

同期間隔 同期サービス	ドメイン マッ	プされた居住 グルー	ブニーザー	セーフガード	
同期するグループを選択します					
フィルタとして使用するトップレベルの レクトリと同期する特定のグループを選	ブループを入力します。 Rします。	・[グループを選択] ポタ	マンをクリックして	、フィルタを適	用し、ディ
✓ ネストされたグループ メンバーを同じ	A				
トップレベル グループを指定	すべてを	同期するグループ			+
グループ DN		マップされたグルー	プ		
				閉じる	保存

[ユーザー] タブを選択します。

● [ユーザー DN を指定] に同期対象の AD ユーザを選択する DN を入力

※[テスト]をクリックして同期対象ADユーザの存在確認ができます。

● [ユーザーを除外するフィルタ...] に同期対象から除外する AD ユーザを指定しま

す。

	명합(A 이원)	サービス ド	*12	マップされた場性 グループ ユーリー	セーフカード	
1期するユーザー?	を選択します。					
ととえば、CN=Us されます。DN で L :N=Users,DC=sal 9を入力します。1	ers,DC=examp LDAP フィルタ es,DC=exampl 司刷から除外す	le,DC=com な。 を使用するには e,DC=com;(&(i るユーザーをす	ど、同期 ? ま、DN に objectClas 旨定する()	するユーザー DN を入力します。DN 配下で見つ セミコロンを追加し、その後に、たとえば、 sa=Useri/objectCategory=Person)(UserAccount には、除外フィルタを使用します。	つかるすべてのユーザ・ (Control=512)) などの:	-も両 フィル
ユーザー DN を指	lê na			20 11 1		+
00= ,DC=	,DC=	,DC=	(objec	tClass=User)	TAP	* +
ユーザーを除外す	るフィルタ					+
ユーザーを除外す name	るフィルタ ン	次を含む	ř	Administrator		+ + ×
ユーザーを除外す name name	でるフィルタ ~ ~	次を含む 次を含む	~ ~	Administrator Guest		+ + × + ×
ユーザーを除外す name name	でるフィルタ ン ン	次を含む 次を含む 次を含む	> > >	Administrator Guest krbtgt		+ +
ユーザーを除外す name name name	るフィルタ 、 、 、	次を含む 次を含む 次を含む	> > >	Administrator Guest krbtgt		+ + + + + +

[保存] をクリックします。

[閉じる] をクリックします。

[同期] > [セーフガードを使用した同期] をクリックすると同期が開始されます。

同期が完了すると、WS1 Access のユーザが登録されます。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

5.2. ID プロバイダの作成

WS1 Access に IdP (ID プロバイダ) を追加します。

Workspace ONE Access コンソール にログインします。

メニュー [統合] > [ID プロバイダ] を選択します。

[ID プロバイダを追加] > [組み込み ID プロバイダを作成] をクリックします。

【組み込み ID プロバイダを追加】

- [ID プロバイダ名] に任意の名前を入力
- [ユーザー] に AD 同期しているディレクトリをチェック
- [コネクタ認証方法] に [パスワード(クラウドデプロイ)] をチェック
- [認証方法] は指定しない。
- [ネットワーク] に [すべての範囲] をチェック

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

ユーザー					
	4				
コネクタ認証方法	認証方法	認証方法を開連付ける			
	ノスワード (クラウド デブロイ)				
認識方法	ID プロバイダがユーザー級証に使用する認証方式を選択します。				
	認証方法	認証方法を翻連付ける			
	VMware Verify				
	モノ(イ)レSSO(IOS 版)				
	パスワード (ローカルディレクトリ)				
	モバイル SSO (Android 版)				
	Workspace ONE UEM の外部アクセス トークン				
	Workspace ONE UEM でのパスワード				
	Workspace ONE UEM とのデバイス開守				
	証明書 (クラウド デブロ・イ)				
ネットワーク	この ID プロバイダにアクセスできるネットワークを選択し	ます。次の利用可能なネットワーク範囲から進択します。			
	✔ すべての範囲				
(DC 証明書のエクスボー	証明書をダウンロード				
r	モバイルデバイス管理プロファイルで使用するための KDC	サーバのルート証明書をエクスポートします。			

[追加] をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

5.3. ユーザーグループの作成

Web アプリケーション (Gléas UA) にアクセスするユーザをグループ化します。

Workspace ONE Access コンソール にログインします。

メニュー [アカウント] > [ユーザーグループ] を選択します。

[グループを追加] をクリックします。

【グループを追加】

● [グループ名] に 任意のグループ名を入力

グループを追加				
グループ名*	a na tina			
説明				
			キャンセル	次へ

[次へ] をクリックします。

● [グループにユーザーを追加] は指定しない

グループにユーザーを追加	
Q、 ユーザーを検索	+
	キャンセル 戻る 次へ

[次へ] をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- 次のルール [すべて] に一致 を選択
- [ディレクトリ] [次であるもの] [AD と同期したディレクトリ] を指定

グループ ルール		
次のルールの すべて	▼ に一致: 人のユーザーが見つかりました	
ディレクトリ	 ▼ 次であるもの 	~ + ×
	キャンセル 戻る	次へ

[次へ] をクリックします。

● [ユーザーをグループから除外] は指定しない

ユーザーをグループから除外	
Q ユーザーを検索	+
	キャンセル 戻る 次へ

[次へ] をクリックします。

設定の確認				
以下を作成しようとして	います:			
グループ名:	17 mar 17 p. 11 mar 144			
除外:	0			
ユーザーの合計数:	すべて表示			
		キャンセル	戻る	グループを作成

[グループを作成]をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

5.4. Web アプリケーションの登録

Web アプリケーション (Gléas UA) を SAML SP として登録します。

Workspace ONE Access コンソール にログインします。

メニュー [リソース] > [Web アプリケーション] を選択します。

[新規] をクリックします。

【定義】

- [名前] に任意のアプリ名を入力
- [説明] に任意のアプリ説明を入力
- [アイコン] に任意のアイコン画像ファイルを選択



[次へ] をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

【シングルサインオン】

- [認証タイプ] に [SAML 2.0] を選択
- [構成] に [手動] を選択
- [シングル サインオン URL] を入力

※https://[UA の FQDN]/ua/[UA の名前]/saml/acs

- [受信先 URL] を入力 ※https://[UA の FQDN]/ua/[UA の名前]/saml/acs
- [アプリケーション ID] を入力
 ※https://[UA の FQDN]/ua/[UA の名前]/saml
- [ユーザー名の形式] に [未指定] を選択
- [ユーザー名の値] に "\${user.userName}" を入力
- [Relay State URL] は指定しない
- [アプリケーション パラメータ] は指定しない
- [高度なプロパティ] リンクをクリック
- [応答に署名] に [はい] を指定
- [アサーションに署名] に [はい] を指定
- [アサーションの暗号化] に [はい] を指定
- [アサーションの署名を含める] に [いいえ] を指定
- [デバイスの SSO の応答] に [いいえ] を指定
- [強制認証要求を有効にします] に [いいえ] を指定

27 / 59

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- [署名アルゴリズム] に [RSA SHA256] を選択
- [ダイジェスト アルゴリズム] に [SHA256] を選択
- [アサーション時間]に "200" を入力
- [署名を要求する] に PEM 形式の SAML SP 署名用証明書を貼付け
- [暗号化証明書] は指定しない
- [認証失敗の通知を有効にする] に [いいえ] を指定
- [アプリケーション ログイン URL] は指定しない
- [プロキシ カウント] は指定しない
- [API アクセス] に [いいえ] を指定
- [カスタム属性マッピング] は 指定しない
- [Workspace ONE Web で開く] に [いいえ] を指定
- [ユーザー ポータルに表示] に [はい] を指定

	シングルサインオン	1.20	
a		2 467	アプリクーション バラメータ ①
アクセスポリシー	54M, 20	· · · · · · · · · · · · · · · · · · ·	Rill - 1889 - 727.01-01 - 01
970	#u2 ° ©	4.970	(728) (728)
	○ URL/XML ◎ 平動		
	0-200 ckch+abcc		ARG70/Gr A
	Higs / Aug /some/acs		2221210E ()
			EU/
	Man / Antifest		アリーションを着名の
	The second se		(1) 180.1
	1004 June June June June June June June June		29-53300045c
			180.
	1 + 8062.0		アリーションの着ちを向めるこ
	A87	×	(M) (M)
	ユ ザ 名の仲の		デル(スの 110 の)(あ 2
	B(user.userhame)		I 14/2
	Relay State URL D		特徴の研究を発見にしたす。①
			(1) 10 m
	welling and the first of a		862670365
	F799-932738-90		RSA SHA251
	名伝・ 御用・ デフォルト信・ 信	-	

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

	タイジェスト 7% 印ズムの		SCF XCSBLRVN, ENEMAgor gYKC2muFyLC0BSRVanNyaClacIMc* ALligation.
200	316250	1 定義	際なな問題の
H.C.		2 H.R	
アクセス ポリシー	79->=>=>=	3 795	
וידי	※名を生まする。() 	4 979	INAROSINGANS / 80 ○■ 1×ス アブリラーション ログイン (RL)
	NHACLERS&⊕		±000+0
	13145.000000000000000000000000000000000000		AN PORAQ
	Star C		0 000
	7207-5151092048-0		カスタム同性マッピング の
			6.00 HTL 60020 10
	7049-5951-0	_	• HT#N
	4P177230		Westman ON White PBC o
	Image: 100 and 100		O 142
	カスタム属性マッピング ①		コーザーボーダルド (東京 () () リン

[次へ] をクリックします。

【アクセスポリシー】

● [default_access_policy_set] を選択

「規 SaaS アプリケー	ション	×
1 定義	アクセス ポリシー	
2 福成	アクセスボリシーは、アプリケーションにアクセスするために満たす必要のある基準を指定します。以下の特定のアプリケ ションへのユーザー アクセスを苦想するには、アクセスボリシーを選択します。	
3 アクセスポリシー	default_access_policy_pet v	
4 サマリ		

[次へ] をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

【サマリ】

定派	定義	
2 構成	6.H	
3 アクセスポリシー	1012	
4 9 7 9		
	243>	
	County In France	
	カデゴリ	
	69/06	
	認証タイプ SAME Z.O	
	退 成	
	于 AD	
	シングル サインオン URL https:// /ua/ /sami/acs	
	受信先 URL	
	https:// /ua/ /sami/acs	
	アプリケーションID http:// /us/ /sami	
	ユーザーをの形式	
	未编定	
	2-9-800	

[保存] をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

5.5. Web アプリケーションの割り当て

作成した Web アプリケーションをユーザーグループに割り当てることで、ユーザが利

用できるようにします。

Workspace ONE Access コンソール にログインします。

メニュー [リソース] > [Web アプリケーション] を選択します。

作成した Web アプリケーションをチェックします。

[割り当て]をクリックします。

【割り当て】

- [選択されたユーザー/ユーザー グループ] に作成したユーザーグループを選択
- [展開の種類]に[ユーザーによるアクティベーション] を選択
- [資格タイプ] に [含める] を選択

訳されたアプリ:	College Co				
ーザー/ユーザー グループ					
2、ユーザーまたはクループを検索					
間沢されたユーザー/ユーザー グループ	原語の視知	資格タイプ	プロビジョニングの状態	再加行	
8	ユーザーによるアクティベーション	<u> </u>	プロビジョニングの状態		×

31 / 59

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

[保存] をクリックします。

※Web アプリケーションは、UA 毎に登録、割り当て、を行う必要があります。PC と iOS などデバイ ス種類ごとに複数の UA を利用している場合などは、それぞれ Web アプリケーションを登録する必要 があります。 シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

6. Gléas の管理者設定 (Windows 向け)

GléasのWindows向けUA(申込局)をWS1AccessのWebアプリケーションとして動作

するように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

画面上部より[認証局]をクリックし認証局一覧画面に移動し、設定を行うUA (申込局)

をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

UA 申込局 ▶ <u>Gleas Generic UA</u> Gleas デフォルト申込局

申込局詳細画面が開くので、基本設定で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- 証明書ストアの選択で、[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]に

チェック

	▶基本設定	
● ダウンロードを許可 ● インボートワンスを利用する ダウンロード可能時間(分) 1 ● 登録済みデバイスのみインボート許可	 □ トークンへのインボート ✓ 証明書ストアへのインボート 	管理するトークン Gemalto .NETカード V 評明まっトアの練舞 ユーザストア V
□ ②抜済みナハイスのみインホート計画 □ ○4証明書本令めたい		 ✓ インボートワンスを利用する ✓ 登録申請を行わない ● 登録申請を行わない
(保存)	□ CA証明書を含めない	□ 豆荻 オウナハコ へのみコノホートs+=」 保存

[上級者向け]をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力

※ https://[WS1 Access の FQDN]/

● [ログアウト URL]を入力

※ https://[WS1 Access の FQDN]/

- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力

※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

● [IdP SSO URL] を入力

※ https://[WS1 Access の FQDN]/SAAS/auth/federation/sso

● [IdP SLO URL] を入力

※ https://[WS1 Access の FQDN]/SAAS/auth/auth/logout

● [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定

※署名用証明書はメタデータ(XML)から取得する ※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

● [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定

※暗号用証明書はメタデータ(XML)から取得する ※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- [ログアウトレスポンスに署名]をチェック
- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

ログイン方法		
🔽 SAML2.0で外部認証する		
ホームURL	https://	.vmwareidentity.asia/
ログアウトURL	https://	.vmwareidentity.asia/
SP Issuer	https://	/ua/ /saml
SP 証明書	□ 削除する	
	★ saml_sp 有効期限:	
SP秘密鍵	□ 削除する	
	黄 あり	
SP ACS URL	https://	/ua/ /saml/acs
SP SLO URL	https://	/ua/ /saml/logout
名前ID形式	urn:oasis:names:tc:SAML:1.1:n	ameid-format:unspecified
IdP エンティティID	https://	.vmwareidentity.asia/SAAS/API/1.0/GET/metai
IdP SSO URL	https://	.vmwareidentity.asia/SAAS/auth/federation/ssc
IdP SLO URL	https://	.vmwareidentity.asia/SAAS/auth/logout
IdP 署名用証明書	🗌 削除する	
	★ VMware Identity Manager 有効期限:	
IdP 暗号用証明書	🗌 削除する	
	★ VMware Identity Manager 有効期限:	
ダイジェストアルゴリズム SHA	4-256 ✔	
署名アルゴリズム RSA SHA	-256 🗸	
☑ 認証リクエストに署名		✓ ログアウトリクエストに署名
 ログアウトレスポンスに署名 ロ 第タネッッセージョー##ゆう3 	2	▼ メタデータに署名
	~	

設定完了後、[保存]をクリックし保存します。

また、認証デバイス設定の以下項目にチェックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android の設定の、[Android 用 UA を利用する]

以上でGléasの設定は終了です。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- 7. クライアントからのアクセス (Windows)
- 7.1. シングルサインオンで UA にログイン

PCのブラウザ (Edge) で、UAのシングルサインオンURLにアクセスします。

※URL https://[UAのFQDN]/ua/[UAの名前]/saml/sso

WS1 Accessのログインページに遷移します。

	Workspace ONE*
Workspace ONE"	ユーザー名 パスワード
ドメインの選択 	ログイン
 この設定を保存 次へ 	バスワードを忘れた場合 別のドメインへ変更
vmware.	vmware

ドメインを選択して[次へ]をクリックします。

[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

Workspace ONE ポータルからログインすることもできます。

	Workspace ONE"
Workspace ONE*	ユーザー名 パスワード
ドメインの選択	······
 この設定を保存 次へ 	ログイン パスワードを忘れた場合
vmware.	別のドメインへ変更 vm ware

ドメインを選択して[次へ]をクリックします。

[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。



[アプリ]タブから登録した「Webアプリケーション」を選択します。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

7.2. クライアント証明書のインポート

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行

われます。

プライベートCA Gléas テスト ユーザ	× +				- 0
\rightarrow C \Box	and the second second second		A	A) 🕼 🙆 🗘	8 🥫 💼
			:	プライベートCA 🤆	léås 🛛
テスト ユーザー さんの	ページ]				■ログアウ
ユーザ情報				_	_
🖉 テスト ユーザーさん	んのページ				
● ユーザ情報					^
▶ ユーザ	登録日時:				
>姓:テスト 名:ユーザー					
>ユーザID:					
> パスワード: ************************************					
> メールアドレス : > バスワード : ***********************************					
★ 証明書情報 ······					
▶ 発行済み証明書					
#	発行局	ジリアル	有効期限	証明書ストアへ・	インボート

※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印 を確認するなど正当性を確認してから[はい]をクリックします

セキュリティ	(警告	\times
<u> </u>	発行者が次であると主張する証明機関 (CA) から証明書をインストールしよ うとしています:	
	証明書が実際に からのものであるかどうかを検証 できません。 に連絡して発行者を確認する必要が あります。次の番号はこの過程で役立ちます: 	
	答告: このルート証明書をインストールすると、この CA によって発行された証明書は 自動的に信頼されます。確認されていない毎印付きの証明書をインストール することは、セキュリティ上、危険です。[はい]をクリックすると、この危険を認 識したことになります。	
	この証明書をインストールしますか?	
	はい(Y) いいえ(N)	

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウ

トさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ロ

Google	🗙 🔟 ブライベートCA Gléas テスト ユーザー 🗙 🕂	-			- 0	
→ C	1		A® 5	à 🧕 🗘		
			プライ	(x-dca Gle	éåš 🛛	
[テスト ユーザー さ	らんのページ]				■ログアウト	
ユーザ情報						
🙎 テスト ユーザ	ーさんのページ					
♥ユーザ情報・					*	L
▶ユーザ	登録日時:					L
>姓:テスト 名:コ	1-17-					L
> ユーザID: > メールアドレス:						L
> バスワード:*******	1******					L
兼証明書情報↔						L
						_
▶ 発行済み証明書						
▶ 発行済み証明書 #	発行局	シリアル	有効期限	証明書ストアヘイン	ポート	

グインしてインポートを行うことはできません。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

8. Gléas の管理者設定 (iPhone 向け)

GléasのiPhone向けUA (申込局) をWS1 AccessのWebアプリケーションとして動作す

るように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA(申込局)

をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

UA 申込局 ▶<u>Gleas Generic UA</u> Gleas デフォルト申込局

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間(分)を経過した後は、

構成プロファイルのダウンロードが不可能になります (インポートロック機能)。これ

により複数台のデバイスへの構成プロファイルのインストールを制限することができま

す。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

▶基本設定	■上級者向け
□ トークンへのインポート	管理するトークン Gemalto .NETカード 🗸
□ 証明書ストアへのインポート	証明書ストアの種類 ユーザストア 🗸
✓ ダウンロードを許可 ダウンロード可能時間(分) 1	 インボートワンスを利用する 登録申請を行わない 登録済みデバイスのみインボート許可
 CA証明書を含めない 	
	保存

[上級者向け]をクリックします。

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力

※ https://[WS1 Access の FQDN]/

● [ログアウト URL]を入力

※ https://[WS1 Access の FQDN]/

- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力

※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

● [IdP SSO URL] を入力

※ https://[WS1 Access の FQDN] /SAAS/auth/federation/sso

● [IdP SLO URL] を入力

※ https://[WS1 Access の FQDN]/SAAS/auth/auth/logout

● [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定

※署名用証明書はメタデータ(XML)から取得する ※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

● [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定

※暗号用証明書はメタデータ(XML)から取得する

※ https://[テナント名].vmwareidentity.asia/SAAS/API/1.0/GET/metadata/idp.xml

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック
- [ログアウトレスポンスに署名]をチェック
- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

ログイン方法		
☑ SAML2.0で外部認証する		
ホームURL	https://	.vmwareidentity.asia/
ログアウトURL	https://	.vmwareidentity.asia/
SP Issuer	https://	/ua/ /saml
SP証明書	🗌 削除する	
	★ saml_sp 有効期限:	
SP 秘密鍵	🗌 削除する	
	🌟 あり	
SP ACS URL	https://	/ua/ /saml/acs
SP SLO URL	https://	/ua/ /saml/logout
名前ID形式	urn:oasis:names:tc:SAML:1.1:n	ameid-format:unspecified
IdP エンティティID	https://	.vmwareidentity.asia/SAAS/API/1.0/GET/meta
IdP SSO URL	https://	.vmwareidentity.asia/SAAS/auth/federation/ssc
IdP SLO URL	https://	.vmwareidentity.asia/SAAS/auth/logout
IdP 署名用証明書	🗌 削除する	
	★ VMware Identity Manager 有効期限:	
IdP 暗号用証明書	🗌 削除する	
	★ VMware Identity Manager 有効期限:	
ダイジェストアルゴリズム SHA	-256 🗸	
署名アルゴリズム RSA SHA-	256 🗸	
☑ 認証リクエストに署名		✓ ログアウトリクエストに署名
 ログアウトレスポンスに署名 アタネッシャー・ジー 埋め込 	5 * `	✓ メタデータに署名
	0	

設定完了後、[保存]をクリックし保存します。

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

用する]をチェックします。

▶ IPhone / IPadの該定	
🗌 iPhone/iPad 用 UA を利用する	

構成プロファイルに必要となる情報の入力画面が展開されるので、以下設定を行います。

【画面レイアウト】

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

【iPhone構成プロファイル基本設定】

● [名前]、[識別子]に任意の文字を入力(必須項目)

🥒 認証デバイス情報・	
▶iPhone / iPadの設定	
🔽 iPhone/iPad 用 UA を利用	利する
画面レイアウト	
 iPhone 用レイアウトを使用 Mac OS X 10.7以降の接 	月する
OTA(Over-the-air)	
 OTAエンロールメントを利用 	用する 📃 接続する iOS デバイスを認証する
OTA用SCEP URL	
OTA用認証局	デフォルトを利用
iPhone 構成プロファイル基	本設定
名前(デバイス上に表示)	サンブルプロファイル
識別子(例: com.jcch-	local.jcch-sss.profile
sss.profile)	
ブロファイルの組織名	JCCHセキュリティ・ソリューション・システムズ
記印	サンブル構成プロファイル

各項目の入力が終わったら、 [保存]をクリックします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

以上でGléasの設定は終了です。

9. クライアントからのアクセス (iPhone)

9.1. シングルサインオンで UA にログイン

iPhoneのブラウザ (Safari) で、UAのシングルサインオンURLにアクセスします。

※URL https://[UAのFQDN]/ua/[UAの名前]/saml/sso

WS1 Accessのログインページに遷移します。

0	
Workspace ONE*	0
ドメインの選択	Workspace ONE"
□ この設定を保存	ユーザー名
次へ	パスワード
	AT 194775 (107-1946) (107
	ログイン
	パスワードを忘れた場合
vmware:	別のドメインへ変更 V m ware

ドメインを選択して[次へ]をクリックします。

[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

Workspace ONE ポータルからログインすることもできます。

0	
Workspace ONE*	0
ドメインの選択	Workspace ONE*
□ この設定を保存	ユーザー名
次へ	バスワード
	10 100 T 10 (11 100) 100
	ログイン
	別のドメインへ変更
vm ware [.]	vmware:

ドメインを選択して[次へ]をクリックします。

[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

Ξ アプリ	
新しいアプリ 💙	Q アプリを検索
すべてのアプリ	
Giess Tervis Tervis	Geess Geess for windows
OfficeS65 Portal	
カテゴリ	

メニュー[アプリ]から登録した「Webアプリケーション」を選択します。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

9.2. クライアント証明書のインポート

[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。

プライベ-	-eca Gléäs 🛯	プラ	51x-fca Gléäs 🛂		プライベートCA Gléä	ÎS UA
テスト ユーザー さん	のページ	テスト ユーザー	- さんのページ	テスト	ユーザー さんのページ	
ユーザロ	100000000000000000000000000000000000000	ユーザID	And Address of Control and Control	ユーザ	D inclusion in	-
姓	テスト	姓	テスト	姓		テスト
名	ユーザー	名	ユーザー	名	ב	ーザー
メール		メール		メール		
NARMANNA TEST CO		このWebサー ウンロードし	イトは構成プロファイルをダ ようとしています。許可し	右効制	プロファイルがダウンロードさ	清泉
有効期限	ダウンロード済み	ますか?			れました	
有効期限	ダウンロード		無視 許可	有幼期	ノロファイルをインストールするには設定 Appで再確認してください。	1-6
Copyright (C) 2010-2022 JCCH Security	ログアウト Solution Systems Co.,Ltd. All rights reserved.	Copyright (C) 2010-2022 JCC	ログアウト 'H Security Solution Systems Co., I M. All rights reserved.	Copyright	閉じる	アフ ^ッ リケト s reserved.

※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

画面の表示にしたがい設定を開くと、プロファイルがダウンロードされた旨が表示され

るので、インストールをおこないます。

設定		キャンセル	プロファイル	インストール
Apple ID、iCloud、メディアと購入	>	بردر انتخاب انتخاب	・ プルプロファイル Hセキュリティ・ソリュー: SAズ	. vev
プロファイルがダウンロード済み	>	Signed by No Description サン Contains 証明	t <mark>Signed</mark> νプル構成プロファイル 月書: 2	
		More Detai	s	>
		Rem	ove Downloaded I	Profile

[インストール]をタップして続行してください。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[インストール]をタップして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります

キャンセル	警告	インストール
管理対象外ルート 証明書 ールすると、if 書のリストに減 定"で有効にす イト用には信頼	^{証明書} Phone にある信 追加されます。 るまで、この記 頁されません。	をインスト 頼できる証明 "証明書信頼設 E明書は Web サ

インストール完了画面になりますので、[完了]をタップして終了します。

	インストール完了	完了
\bigcirc	サンプルプロファイル JCCHセキュリティ・ソリューション・ システムズ	
Signed by Description Contains	Not Signed サンプル構成プロファイル 証明書: 2	
More De	etails	>

なお [More Details]をタップすると、インストールされた証明書情報を見ることがで

きます。必要に応じて確認してください。

く 戻	3	サンプルプロファイル	
11	[明書	(2)	
1	⊗		>
1	0	発行元: 有効明限:	>

Safariに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、iPhoneでの構成プロファイルのインストールは終了です。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より 管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロ ード済み」という表記に変わり、以後のダウンロードは一切不可となります。

プライ	x-dca Gléäs 🛛
テスト ユーザー さ	んのページ
ユーザID	
姓	テスト
名	ユーザー
メール	
有効期限	ダウンロード済み
有効期限	ダウンロード済み
	ログアウト
Copyright (C) 2010-2022 JCCH Sec	arity Solution Systems Co.,Ltd. All rights reserved

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

10.Gléas の管理者設定 (Android 向け)

GléasのAndroid向けUA (申込局) をWS1 AccessのWebアプリケーションとして動作す

るように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA(申込局)

をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

UA 申込局 ▶<u>Gleas Generic UA</u> Gleas デフォルト申込局

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間(分)を経過した後は、

証明書ファイルのダウンロードが不可能になります (インポートロック機能)。これに

より複数台のデバイスへの証明書ファイルのインストールを制限することができます。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

□ トークンへのインボート 管理するトークン Gemaito.NETカードマ □ 証明書ストアへのインボート 証明書ストアの種類 ユーザストア ② ダウンロードを許可 ダウンロード可能時間(分) 1 ○ 登録申請を行わない ○ 登録申請を行わない ● 登録を消あたりレイスのみインボード許可
 CA証明書を含めない (保存)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力

※ https://[WS1 Access の FQDN]/

● [ログアウト URL]を入力

※ https://[WS1 Access の FQDN]/

- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力

※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

● [IdP SSO URL] を入力

※ https://[WS1 Access の FQDN]/SAAS/auth/federation/sso

● [IdP SLO URL] を入力

※ https://[WS1 Access の FQDN]/SAAS/auth/auth/logout

● [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定

※署名用証明書はメタデータ(XML)から取得する ※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

● [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定

※暗号用証明書はメタデータ(XML)から取得する

※ https://[WS1 Access の FQDN]/SAAS/API/1.0/GET/metadata/idp.xml

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック
- [ログアウトレスポンスに署名]をチェック
- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

ログイン方法		
🔽 SAML2.0で外部認証する		
ホームURL	https://	.vmwareidentity.asia/
ログアウトURL	https://	.vmwareidentity.asia/
SP Issuer	https://	/ua/ /saml
SP証明書	□ 削除する	
	★ saml_sp 有効期限:	
SP 秘密鍵	□ 削除する	
	兼 あり	
SP ACS URL	https://	/ua/ /saml/acs
SP SLO URL	https://	/ua/ /saml/logout
名前ID形式	urn:oasis:names:tc:SAML:1.1:r	nameid-format:unspecified
IdP エンティティID	https://	.vmwareidentity.asia/SAAS/API/1.0/GET/metai
IdP SSO URL	https://	.vmwareidentity.asia/SAAS/auth/federation/ssc
IdP SLO URL	https://	.vmwareidentity.asia/SAAS/auth/logout
IdP 署名用証明書	□ 削除する	
	★ VMware Identity Manager 有効期限:	
IdP 暗号用証明書	□ 削除する	
	★ VMware Identity Manager 有効期限:	
ダイジェストアルゴリズム SHA	4-256 ✔	
署名アルゴリズム RSA SHA	-256 🗸	
☑ 認証リクエストに署名		☑ ログアウトリクエストに署名
■ ログアウトレスポンスに署約	2 +.	☑ メタデータに署名
□ 者名をメッセージに理め込	1. C.	

設定完了後、[保存]をクリックし保存します。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

[認証デバイス情報]の[Androidの設定]までスクロールし、[Android用UAを利用する]を

チェックします。

▶ Android の設定
Android 用 UAを利用する
ダウンロードの動作
 □ ログインパスワードで証明書を保護 ☑ 数字のみの PIN を表示 証明書ダウンロードの種類 □ PKCS#12ダウンロード
保存

証明書のダウンロードに必要となる情報の入力画面が展開されるので、以下設定を行い

ます。

- [数字のみのPINを表示]をチェック
- [証明書ダウンロードの種類]]を[PKCS#12ダウンロード]を選択

各項目の入力が終わったら、 [保存]をクリックします。

プライベー	ト認証局	Gléas ホワイ	トペーパー
-------	------	-----------	-------

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

証明書インポートアプリ CertImporter for Android を使用する場合は、[証明書インポ

ートアプリ連携の設定] までスクロールし、[証明書インポートアプリを利用する]をチェ

ックします。

▶証明書インボートアブリ連打	携の設定		
 ☑ 証明書インボートアブリを計 インボートボタンを表示 証明書一覧をアブリで表示 証明書と一緒こUAマニフっ 証明書と一緒こUAマニフっ 証明書PINをGléasで生成 	川用する (MacOSXのみ) ・ストをダウンロード		
UAマニフェスト			
ログインURL			
信頼するCA証明書	ファイルの選択ファイルが選択されていません		
<u>UAマニフェスト要求ファイル</u> を	ダウンロードして、弊社サポートに送付してください		
UAマニフェストのアップロード ファイルの選択 ファイルが選択されていません			
	保存		

入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

11. クライアントからのアクセス (Android)

11.1. シングルサインオンで UA にログイン

Androidのブラウザ (Chrome) で、UAのシングルサインオンURLにアクセスします。

※URL https://[UAのFQDN]/ua/[UAの名前]/saml/sso

WS1 Accessのログインページに遷移します。

۵	0
Workspace ONE*	Workspace ONE*
ドメインの選択	ユーザー名
v	パスワード
□ この設定を保存	
次へ	p171001775.p175-000.000
	ログイン
	ログイン パスワードを忘れた場合
	ログイン パスワードを忘れた場合 別のドメインへ変更
	ログイン パスワードを忘れた場合 別のドメインへ変更
	ログイン パスワードを忘れた場合 別のドメインへ変更
	ログイン パスワードを忘れた場合 別のドメインへ変更

ドメインを選択して[次へ]をクリックします。

[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

Workspace ONE ポータルからログインすることもできます。

\bigcirc	0
Workspace ONE*	Workspace ONE"
ドメインの選択	ユーザー名
□ この設定を保存	
	201 Hold T. D. (1990) 1990 1990
	ログイン
	パスワードを忘れた場合
	別のドメインへ変更
vmware [.]	vmware [.]

ドメインを選択して[次へ]をクリックします。

[ユーザー名]、[パスワード]を入力して[ログイン]をクリックします。

≡ アプリ		
新しいアプリ * Q アブリを検索		
すべてのアプリ		
75 re-sca Glétis III fer Antroid	Generation Generation for los	
Web サイト 🛈 🏠	Web サイト 🕡 🏠	
Gléži III Gléži III for Windows	Office365 Portal	
Web サイト 访 🏠	Web サイト 访 🏠	
カテゴリ		

メニュー [アプリ]から登録した「Webアプリケーション」を選択します。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

11.2.クライアント証明書のインポート

[ダウンロード]をタップし、証明書ファイルのダウンロードをおこないます。

JETA-FCA Gléäs UA		プライベ	-eca Gléäs ua	プライベート	ca Gléäs ua
テスト ユーサ	ザー さんのページ	テスト ユーザー さんの)ページ	テロションを加出	
ユーザID		ユーザID		証明書を抽出するためのパ	n スワードを入力しま
姓	テスト	姓	テスト	\$ \$_	
名	ユーザー	名	ユーザー	4	·
メール		メール		2	
				N	ヤンセル OK
有効期限	ダウンロード	証明書 PIN:	決定 キャンセル	有効期限	ダウンロード
	ログアウト		ログアウト		ログアウト
Copyright (C) 2010-202 reserved.	2 JCCH Security Solution Systems Co.,Ltd. All rights	Copyright (C) 2010-2022 JCCH Security reserved.	Solution Systems Co.,I.td. All rights		

※ 「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。

※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

[OK]をタップして続行してください。

「証明書の種類の用途」のダイアログが出るので、用途を選択します。

×	証明書の種類の選択	
7	 VPN とアプリユーザー証明書 Wi-Fi 証明書 	۲ ۲
Cor reso	キャンセル	ОК

[OK]をタップして続行してください。

N	この証明書の名前ない	を指定してく	ださ	
7	証明書名 			37
Cor res		キャンセル	ОК	

[OK]をタップします。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

Chromeに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、Androidでの証明書ファイルのインストールは終了です。

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

[設定]>[セキュリティ]>[詳細設定]>[暗号化と認証情報]>[ユーザー認証情報]>[証明書 の名前]とタップすると、インストールされた証明書情報を見ることができます。必要 に応じて確認してください。



なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より 管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロ ード済み」という表記に変わり、以後のダウンロードは一切不可となります。

プライベ	-pca Gléäs 🛯	
テスト ユーザー さんのページ		
ユーザID		
姓	テスト	
名	ユーザー	
メール		
有効期限	ダウンロード済み	
有効期限	ダウンロード済み	
Copyright (C) 2010-2022 JCCH Securi	ログアウト ty Solution Systems Co.,Ltd. All rights reserved.	

シングルサインオンによる Gléas UA ログイン (VMware Workspace ONE Access 連携)

12.問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや本検証内容、テスト用証明書の提供に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 050-3821-2195

Mail: sales@jcch-sss.com